IN THE CLAIMS:

Please amend claims 14, 20-23, 25, 27-29 and 31-39 as follows.

1. (Cancelled)

2. (Previously Presented) A method according to claim 14, wherein said interception gateway element is integrated in said second network element.

3. (Previously Presented) A method according to claim 14, wherein a header of a data packet is read by said second network element and data packets to be intercepted are duplicated.

4. (Previously Presented) A method according to claim 14, wherein said intercepted data packet is transmitted to said interception gateway element using a secure tunnel.

5. (Original) A method according to claim 4, wherein said secure tunnel is implemented by an encryption processing.

6. (Previously Presented) A method according to claim 14, wherein said intercepted data packet is transmitted via interworking units and encrypted between said interworking units, when said first network element and said interception gateway element are arranged in separate network segments.

7. (Previously Presented) A method according to claim 14, wherein said first network element is provided in each network segment of said packet network.

8. (Previously Presented) A method according to claim 14, wherein received intercepted data packets are collected in said interception gateway element and supplied to an interface of said at least one intercepting authority.

9. (Original) A method according to claim 8, wherein said interface comprises a first interface for administrative tasks, a second interface for network signaling, and a third interface for intercepted user data.

10. (Previously Presented) A method according to claim 14, wherein said intercepting function comprises a packet sniffing and filtering function.

11. (Previously Presented) A method according to claim 10, wherein said intercepting function is implemented in a Gn interface.

12. (Previously Presented) A method according to claim 14, wherein said interception function comprises reading data packets, analyzing the header of the data packets as to whether the data packet should be intercepted or not, and transmitting the data packet to said interception gateway element, and a management function for interception and transmission criteria.

13. (Previously Presented) A method according to claim 14, wherein an alarm is transmitted to said interception gateway element and all interception information of a respective network element is deleted, when a breakage of a casing of the respective network element has been detected.

14. (Currently Amended) An interception method for performing a lawful interception in a packet network, comprising ~~the steps of~~:

~~a)~~ providing a first network element having an interception function for intercepting data packets;

~~b)~~ controlling said interception function by an interception control means implemented in a second network element; and

e) ——transmitting an intercepted data packet from said first network element via said packet network to an interception gateway element providing an interface to at least one intercepting authority, wherein said first network element generates fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said first network element to said interception gateway element,

wherein said fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant.

15. (Cancelled)

16. (Previously Presented) A method according to claim 14, wherein said intercepted data packet is padded to a maximum length.

17. (Previously Presented) A method according to claim 14, wherein a time information is added to said intercepted data packet.

18. (Cancelled)

19. (Previously Presented) A system according to claim 21, wherein said second network element corresponds to said interception gateway element.

20. (Currently Amended) A system according to claim 21, wherein said first network element further comprises an encrypting unit configured to encrypt ~~means for encrypting~~ said intercepted data packet.

21. (Currently Amended) An interception system ~~for performing a lawful interception in a packet network,~~ comprising:

~~a)~~ a first network element having an interception function ~~for intercepting~~ to intercept data packets and comprising a transmitting unit configured to transmit ~~means for transmitting~~ an intercepted data packet to said packet network;

~~b)~~ an interception control unit ~~means~~ implemented in a second network element and ~~controlling~~ configured to control the interception function; and

~~c)~~ an interception gateway element having a receiving unit ~~means for receiving~~ configured to receive said intercepted data packet and an interface unit configured to provide ~~means for providing~~ an interface to at least one intercepting authority,

wherein said first network element further comprises a ~~means for~~ generating unit configured to generate fake packets to be transmitted with said intercepted data packets, and

wherein said transmitting unit is further configured to transmit ~~means transmits~~ said fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant,

wherein the interception system is configured to perform a lawful interception in a packet network.

22. (Currently Amended) A system according to claim 21, wherein said first network element comprises a reading unit configured to read ~~means for reading~~ a header of a received data packet and for duplicating a data packet to be intercepted.

23. (Currently Amended) A system according to claim 22, wherein said reading unit means is configured ~~arranged~~ to pad said copied data packet to a maximum length.

24. (Previously Presented) A system according to claim 21, wherein said first network element is a gateway element of said packet network.

25. (Currently Amended) A system according to claim 21, wherein said first network element is a ~~BG~~ border gateway, an serving GPRS support node ~~SGSN~~ or a ~~GGSN~~ gateway GPRS support node.

26. (Previously Presented) A system according to claim 24, wherein an interception information defining a data packet to be intercepted is included in a context information supplied to said first network element and used for routing data packets.

27. (Currently Amended) A system according to claim 26, wherein said interception control ~~means~~ unit further comprises a storing unit configured to store ~~means for storing~~ an interception list, and wherein said interception control unit ~~means~~ is ~~arranged~~ configured to add said interception information to said context information supplied to said first network element.

28. (Currently Amended) A system according to claim 21, wherein said first network element is ~~arranged~~ configured in each segment of said packet network.

29. (Currently Amended) A system according to claim 21, wherein said first network element comprises a control unit ~~means for controlling~~ configured to control interception and encryption processing in accordance with an interception setting instruction received from said interception control means.

30. (Cancelled)

31. (Currently Amended) An interception system ~~for performing a lawful interception in a packet network,~~ comprising:

~~a)~~ ——a first network element having an interception function for intercepting data packets and comprising a transmitting unit configured to transmit ~~means for transmitting~~ an intercepted data packet to said packet network;

~~b)~~ ——an interception control unit ~~means~~ implemented in a second network element and further configured to control ~~controlling~~ the interception function; and

~~c)~~ ——an interception gateway element having a receiving unit configured to receive ~~means for receiving~~ said intercepted data packet and an interface unit configured to provide ~~means for providing~~ an interface to at least one intercepting authority, wherein said interception gateway element comprises a memory unit configured to store ~~means for storing~~ received intercepted data packets before supplying them to said interface unit ~~means~~,

wherein said interception gateway element comprises a decryption unit configured to remove ~~means for removing~~ an encryption of the received intercepted data packets, an extraction unit configured to extract ~~means for extracting~~ intercepted data packets from fake data packets, and an ~~means for~~ adding unit configured to add a time

information to said received intercepted data packets before storing them in said memory unit ~~means~~, and

wherein said transmitting unit is further configured to transmit ~~means transmits~~ said fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant,

wherein the interception system is configured to perform a lawful interception in the packet network.

32. (Currently Amended) A system according to claim 21, wherein said first network element comprises a detecting unit configured to detect ~~means for detecting~~ a malfunction and/or breakage thereof, and signaling unit configured to signal ~~means for signaling~~ an alarm to said interception gateway element in response to an output of said detecting unit ~~means~~.

33. (Currently Amended) A network element for a packet network, comprising:

~~a)~~ an interception unit ~~means for intercepting~~ configured to intercept a data packet received from said packet network, and

~~b)~~ a transmitting unit configured to transmit ~~means for transmitting~~ said intercepted data packet via said packet network to an interception gateway element,

~~c)~~ wherein said interception unit ~~means~~ is controlled by an interception control unit configured ~~means arranged~~ in another network element, and said network

element further comprises a ~~means for~~ generating unit configured to generate fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said network element to said interception gateway element, and

wherein said fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant.

34. (Currently Amended) An interception gateway element for an interception system of a packet network, comprising:

~~a)~~ a receiving unit configured to receive ~~means for receiving~~ an intercepted data packet via said packet network from a network element having an interception function;

~~b)~~ an interface unit configured to provide ~~means for providing~~ an interface to an intercepting authority;

~~c)~~ a memory unit configured to store ~~means for storing~~ received intercepted data packets before supplying them to said interface unit ~~means~~ wherein said interception gateway element comprises a decryption unit configured to remove ~~means for removing~~ an encryption of the received intercepted data packets, an extraction unit configured to extract ~~means for extracting~~ intercepted data packets from fake data packets and an ~~means for~~ adding unit configured to add a time information to said received intercepted data packets before storing them in said memory.

wherein said receiving unit is further configured to receive ~~means receives~~ said fake packets transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets received by said interception gateway element is constant.

35. (Currently Amended) An interception gateway element according to claim 34, further comprising an interception control unit configured to control ~~means for controlling~~ said interception function of said network element.

36. (Currently Amended) An interception system ~~for performing a lawful interception in a packet network,~~ comprising:

~~a)~~ ——a first network element having an interception function for intercepting data packets and comprising a transmitting means for transmitting an intercepted data packet to ~~said~~ a packet network;

~~b)~~ ——an interception control means ~~unit~~ implemented in a second network element, ~~wherein the interception control unit is configured to control~~ for controlling the interception function; and

~~c)~~ ——an interception gateway element having a receiving means for receiving ~~unit configured to receive~~ said intercepted data packet and an interface unit ~~configured to provide~~ for providing an interface to at least one intercepting authority,

wherein said first network element ~~is~~ further includes ~~further configured to~~ a generating means for generating ~~generate~~ fake packets to be transmitted with said intercepted data packets, and

wherein said transmitting means ~~unit~~ is further configured ~~to transmit~~ for transmitting said fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant,

wherein the interception system is configured for performing a lawful interception in the packet network.

37. (Currently Amended) An interception system ~~for performing a lawful interception in a packet network,~~ comprising:

~~a)~~ a first network element having an interception function for intercepting data packets and comprising a transmitting means for transmitting an intercepted data packet to ~~said~~ a packet network;

~~b)~~ an interception control means ~~unit~~ implemented in a second network element and configured ~~to control~~ for controlling the interception function; and

~~c)~~ an interception gateway element having a receiving means for receiving ~~unit configured to receive~~ said intercepted data packet and an interface means for providing ~~unit configured to provide~~ an interface to at least one intercepting authority,

wherein said interception gateway element comprises a memory means for storing ~~unit configured to store~~ received intercepted data packets before supplying them to said interface means ~~unit~~,

wherein said interception gateway element comprises a decryption means for removing an encryption of the received intercepted data packets, an extraction means for extracting intercepted data packets from fake data packets, and a means for adding a time information to said received intercepted data packets before storing them in said memory means, and

wherein said transmitting means transmits said fake packets at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant,

wherein the interception system is configured for performing a lawful interception in the packet network.

38. (Currently Amended) A network element for a packet network, comprising:

~~a)~~ an interception means ~~unit configured to intercept~~ for intercepting a data packet received from said packet network, and

~~b)~~ a transmitting means ~~unit configured to transmit~~ for transmitting said intercepted data packet via said packet network to an interception gateway element,

~~c)~~ wherein said interception means ~~unit~~ is controlled by an interception control means ~~unit~~ in another network element, and said network element ~~is~~ further

~~configured to generate~~ means for generating fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said network element to said interception gateway element, and

wherein said fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant.

39. (Currently Amended) An interception gateway element ~~for an interception system of a packet network,~~ comprising:

~~a)~~ a receiving ~~unit~~ means ~~configured to receive~~ for receiving an intercepted data packet via ~~said~~ a packet network from a network element having an interception function;

~~b)~~ an interface means ~~unit configured to provide~~ for providing an interface to an intercepting authority;

~~c)~~ a memory means ~~unit configured to store~~ for storing received intercepted data packets before supplying them to said interface means ~~unit~~ wherein said interception gateway element comprises a decryption means for removing ~~unit configured to remove~~ an encryption of the received intercepted data packets, an extraction means for extracting ~~unit configured to extract~~ intercepted data packets from fake data packets and a adding means ~~unit configured to add~~ for adding a time information to said received intercepted data packets before storing them in said memory means unit.

wherein said receiving means ~~unit~~ is further configured for receiving ~~to receive~~ said fake packets transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets received by said interception gateway element is constant,

wherein the interception gateway element is configured for an interception system of the packet network.